

2014 年 HIRT 活動報告

HIRT: Annual Report 2014

Hitachi Incident Response Team (HIRT)
<http://www.hitachi.co.jp/hirt/>

〒140-8573 東京都品川区南大井 6-26-2 大森ベルポート B 館
 OMORI BELLPORT Tower B, 6-26-2 Minamioi, Shinagawa, Tokyo, Japan 140-8573

1 はじめに

振り返れば、2014 年は脆弱性対策の再考の年であった。

Heartbleed, Shellshock, POODLE. 脆弱性に付与された別名である。2014 年は、広範囲に影響を与え、注目を集めた脆弱性が報告された (表 1)。

CVE-2014-10001. 新番号体系で付与された共通脆弱性識別子である。2014 年 1 月 1 日から、プログラム自身に内在するプログラム上のセキュリティ問題に一意の番号を付与する共通脆弱性識別子 CVE (Common Vulnerability and Exposures) の番号体系が更新され、年間上限の制約がなくなった (表 2)。

7,937. NVD に登録された共通脆弱性識別子の件数である。代表的な脆弱性対策データベースの登録件数は、脆弱性のカウント単位が異なるために件数の差異は見られるものの、増加傾向にある (図 1)。

表 1 : 2014 年に報告された代表的な脆弱性

時期	概要
2014 年 1 月	UDP を用いた増幅攻撃 (リフレクター攻撃)
2014 年 4 月	Heartbleed OpenSSL Heartbeat 拡張の脆弱性 (CVE-2014-0160)
	Apache Struts ClassLoader の操作を許してしまう脆弱性 (CVE-2014-0094, CVE-2014-0112, CVE-2014-0113, CVE-2014-0114, CVE-2014-0116)
	マイクロソフト Internet Explorer の脆弱性 (CVE-2014-1776)
2014 年 9 月	Shellshock GNU bash の脆弱性 (CVE-2014-6271, CVE-2014-7169, CVE-2014-6277, CVE-2014-6278)
2014 年 10 月	POODLE SSL 3.0 の脆弱性 (CVE-2014-3566)
2014 年 11 月	マイクロソフト Schannel の脆弱性 (CVE-2014-6321)

表 2 : CVE の新番号体系

旧番号体系	新番号体系
CVE-YYYY-NNNN	CVE-YYYY-NNNN.....N
NNNN は 4 桁固定 年間上限が 9,999 件	NNNN.....N は桁数可変 ただし、1~999 は 4 桁固定 年間上限なし
CVE-1999-0067 CVE-2005-4873 CVE-2012-0158	CVE-2014-0123 CVE-2014-54321 CVE-2014-456132 CVE-2014-7654321

2014 年は、情報システムや制御システムをベースにインターネットを活用して構築された社会インフラが、インシデントにつながる脅威の一つとして、脆弱性という課題に直面していることを浮かび上がらせた。そして、日々のサイバー対策活動を通して、新たな脅威と成り得る脆弱性という課題に立ち向かっていく必要があることを示唆した。この認識の広がりには、インシデント対応という活動の中に、事案が発生した後の活動である事後対応(Response)だけではなく、事案につながる可能性を除去するための脆弱性対策という事前対応 (Readiness) を含み始めたと言える。

CSIRT (Computer/Cyber Security Incident Response /Readiness Team) としての HIRT (Hitachi Incident Response Team) の具体的な役割は、『脆弱性対策：サイバーセキュリティに脅威となる脆弱性を除去するための活動』と『インシデント対応：発生しているサイバー攻撃を回避並びに解決するための活動』を通じて、日立グループのサイバーセキュリティ対策活動を先導していくことに変わりはない。

また、我々の考える CSIRT の要件は、脆弱性対策やインシデント対応を推進するにあたり、『技術的な視点で脅威を押し量り、伝達できること』、『技術的な調整活動ができること』、『技術面での対外的な協力ができること』という能力を備えていることである。

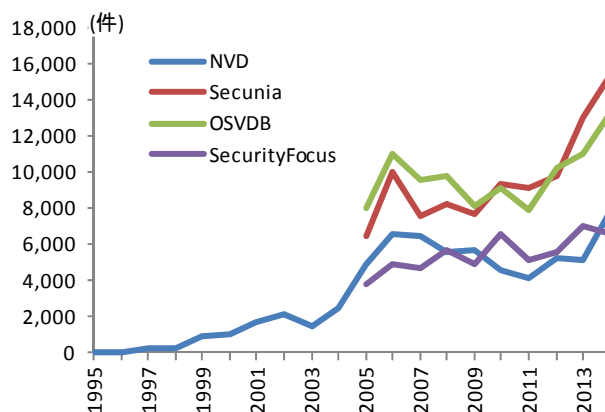


図 1 : 脆弱性対策データベースの登録件数

これは、特別な要件を想定しているわけではない。インシデントオペレーション（インシデントに伴う被害を予測ならびに予防し、インシデント発生後は被害の拡大を低減するために実施する一連のセキュリティ対策活動）の経験値を活かして『次の脅威をキャッチアップする過程の中で早期に対策展開を図る』ことにある。HIRTは、これら能力ならびに役割を持った組織として、製品ならびにサービスの脆弱性対策、マルウェア被害や情報漏洩などのインシデント対応を先導すると共に、日立グループのCSIRT統一窓口組織としての役割を担っている。

本稿では、2014年のHIRT活動の報告として、2014年の脅威と脆弱性の概況、HIRTの活動トピックスについて報告する。

2 2014年の活動概要

本章では、2014年の脅威と脆弱性の概況、HIRTの活動を報告する。

2.1 脅威と脆弱性の概況

(1) 脅威の概況

標的型攻撃、Webサイトの侵害など、既知の脅威による被害は継続している状況にある。

2014年のインシデントの特徴としては、インターネットバンキングを対象とした不正プログラムによる被害の深刻化が挙げられる。一方、攻撃手法としては、パソコン内のファイルを人質にとるランサムウェアの台頭、アカウント情報を辞書化して様々なサイトに不正ログインを試みて個人情報などの閲覧等を行うパスワードリスト攻撃、要求/応答のメッセージ増幅を利用した増幅攻撃（いわゆる、リフレクター攻撃）の定常化が挙げられる。

● インターネットバンキングを対象とした不正プログラムによる被害

警察庁の報告によれば、2014年の国内の不正送金被害は計1,876件（2013年の1.4倍）、被害総額は約29億1,000万円（2013年の2倍）に上っている（図2）[1]。特徴としては、法人名義口座に係る被害が拡大し、不正送金処理を自動で行う不正プログラムの利用手口が悪質ならびに巧妙化している。

● Webサイト侵害活動の定常化

2013年3月以降、国内Webサイトでは、ホームページ誘導型マルウェア感染を意図したページ改ざん事案が続いている。報告件数を見ると、2009年に発生したガンブラー（Gumblar）事案のときよりも、多くの改ざんが発生している状況は継続している（図3）。

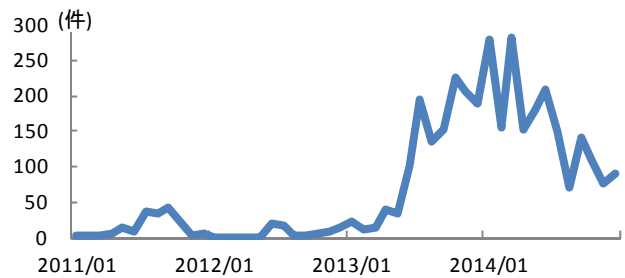


図 2：不正送金事案の月別被害件数
（出典：警察庁）

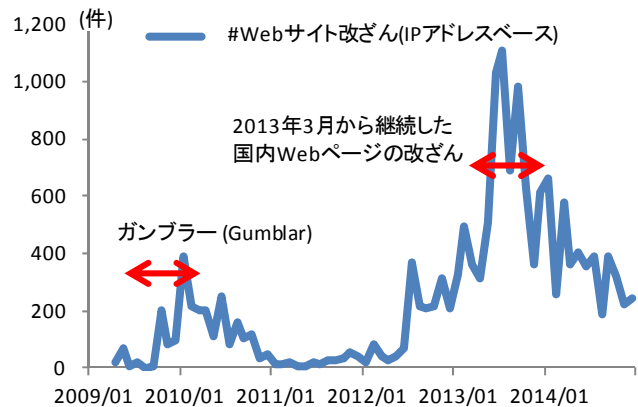


図 3：Webサイトのページ改ざんの報告件数
（出典：JPCERT/CC）

特に、古いバージョンのコンテンツ管理システム（Wordpress, Movable Type, Joomla!, Drupal など）やそのプラグインの脆弱性が悪用され侵害に至っている。

● ランサムウェア

ランサムウェアは、パソコン内のファイルを人質にとる不正プログラムの総称である。シマンテックの報告によれば、2014年は880万（2013年の2.1倍）で、特に、パソコン内のファイルを暗号化し、その暗号解除と引き換えに金銭を要求するランサムウェアは37.3万（2013年の45倍）に急増している[2]。

情報搾取に比べ、影響を受けたファイルを特定はしやすいが、重要なファイルがランサムウェアによって暗号化されてしまった場合には、事業継続に直接的影響を与える可能性がある。サイバー攻撃対策も情報搾取だけではなく、情報破壊にも目を向けていく必要がある。

● パスワードリスト攻撃（リスト型攻撃）

公表情報を元に集計したパスワードリスト攻撃の国内での報告件数を図4に示す。2013年4月以降、何らかの手段で入手した他者のアカウント情報（IDとパスワード）一覧を辞書化した後、これらアカウント情報一覧の辞書を使って、不正ログインを試みる事案は継続している。

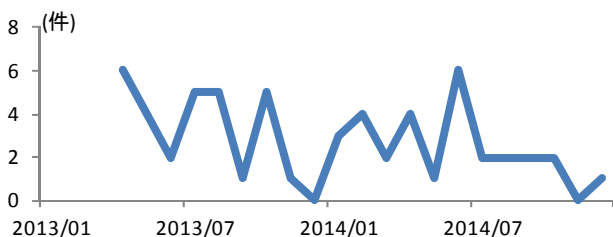


図 4：パスワードリスト攻撃に関する報告件数

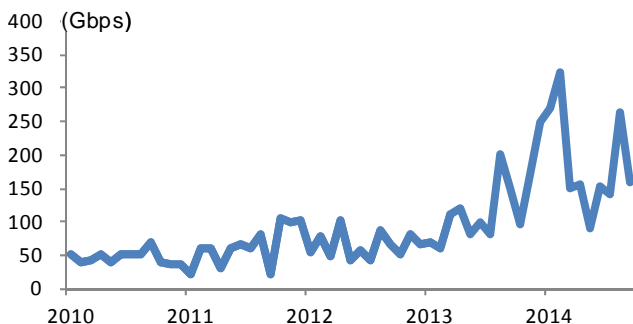


図 5：DDoS 攻撃のピークトラフィックの推移 (出典：Arbor Networks) [3]

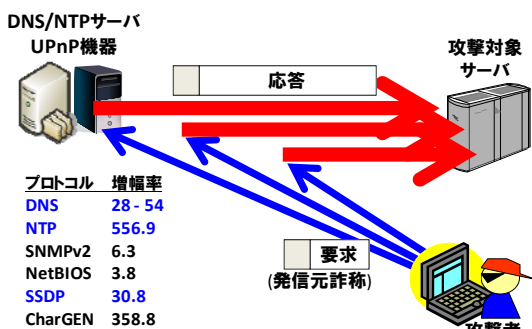


図 6：リフレクター攻撃

● リフレクター攻撃

DDoS 攻撃のピークトラフィックは増加傾向にあり (図 5)，DDoS 攻撃の脅威は継続している。2013 年に顕在化した発信元 IP アドレスを詐称し、踏み台となる要求/応答のメッセージ増幅率の高い (= 応答サイズ ÷ 要求サイズの値が大きい) サービスにパケットを送信する攻撃手法である DrDoS (Distributed Reflective Denial of Service, 分散リフレクター型のサービス不能) 攻撃については、2014 年に入ってから DNS サーバ (オープンリゾルバ) と NTP サーバに加え、UPnP (Universal Plug and Play) 対応機器の SSDP (Simple Service Discovery Protocol) プロトコルを用いた攻撃が報告され始めた (図 6)。

(2) 脆弱性の概況

● 全体傾向

米 NIST NVD (National Vulnerability Database) [4] に登録された 2014 年の脆弱性の総件数は 7,937 件である。このうち、Web 系ソフトウェア製品の脆弱性が約 2 割 (1,768 件) を占めており (図 7)、内訳は、クロスサイト・スクリプティング (XSS)、SQL インジェクションが約 8 割を占めるという状況が続いている (図 8)。同じく、IPA に報告された稼動中 Web サイトの脆弱性のうち、約 6 割がクロスサイト・スクリプティング (XSS)、SQL インジェクションによって占められており、これら脆弱性の報告件数も 600 件/年近くが続いている状況にある (図 9) [5]。

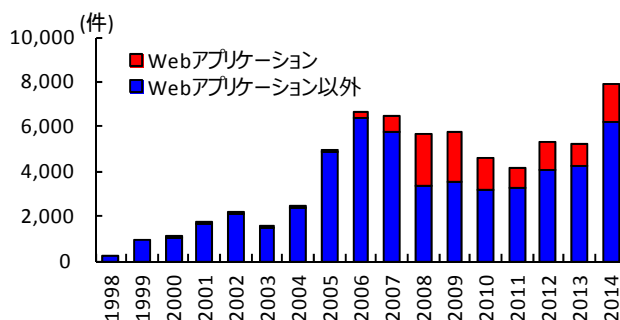


図 7：脆弱性報告件数の推移 (出典：NIST NVD)

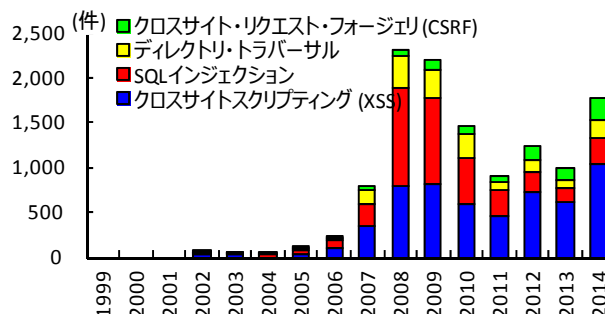


図 8：Web 系ソフトウェア製品の脆弱性報告件数の推移 (出典：NIST NVD)

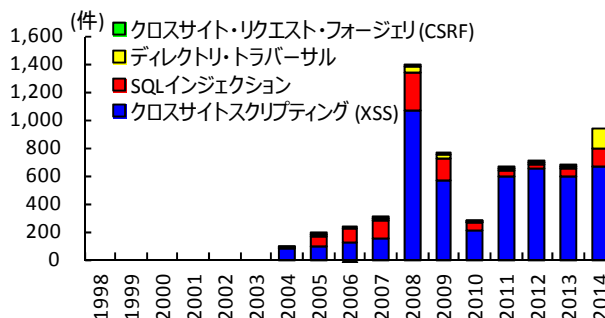


図 9：Web サイトの脆弱性報告件数の推移 (出典：IPA, JPCERT/CC)

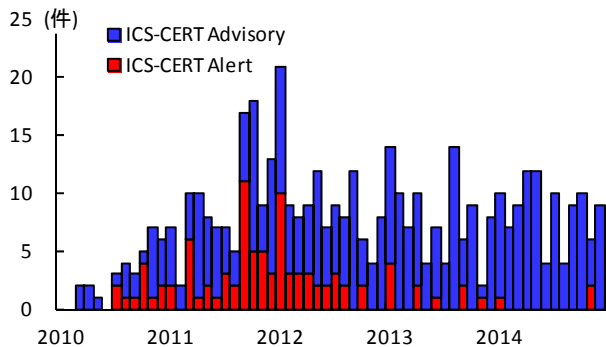


図 10: 制御システム製品の脆弱性報告件数の推移 (出典: ICS-CERT)

● 制御システム製品

米 ICS-CERT (Industrial Control System-CERT) から発行された注意喚起 (Alert) とアドバイザリはそれぞれ 3 件, 99 件である (図 10). アドバイザリのうち, 入力データの検証が適切ではないこと (CWE-20) に起因する脆弱性が 16 件, スタックバッファオーバーフロー (CWE-121) に起因する脆弱性が 13 件となっている. また, 電力および水道施設などで使用される通信プロトコル DNP3 (Distributed Network Protocol) を実装する製品の脆弱性に関するものが 10 件 (2013 年は 15 件) 報告された.

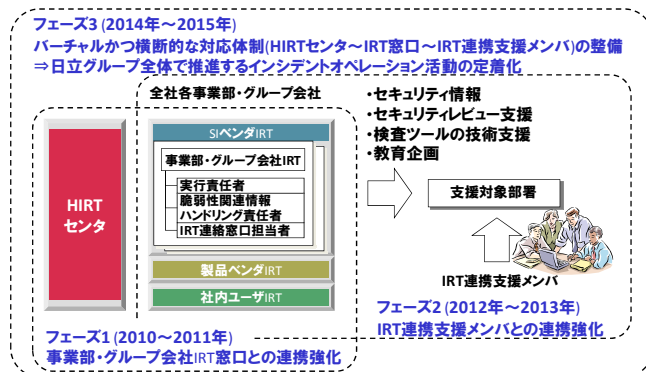
2.2 HIRT の活動トピックス

(1) 日立グループ CSIRT 活動の向上 (フェーズ 3)

2010 年, 『日立グループ全体にインシデントオペレーション活動を浸透させていくこと』を目標として日立グループ CSIRT 活動の向上を開始した (図 11). 5 年目となる 2014 年は, フェーズ 3 の開始年として, HIRT ラボプロジェクトルームを横浜研究所の施設内に開設した. このプロジェクトルームは, 技術継承の場であり, 支援活動ならびに研究所との協働の拠点として活用することを目的としている. 2014 年は, サイバー攻撃で使用されるマルウェアなどの解析の技術継承を目的とする機器を導入した. プロジェクトルームを用いた技術継承については, HIRT オープンミーティング『技術編』と連携しながら, サイバー攻撃で使用されるマルウェアなどの動作の『解析』, 記録された痕跡から事象を把握する『調査』を推進した (表 3) [*a].

*a) HIRT オープンミーティング

信頼関係に基づく HIRT コミュニティを普及させるための活動. 『HIRT 活動に関して, HIRT センタに所属するメンバー同士が情報交換する場である』『HIRT センタの活動内容について, 日立グループに広く知ってもらふことと, HIRT センタ以外からの意見を広く取り入れるために, 情報交換する場を公開する』『公開の場を通じて, 信頼関係に基づく HIRT コミュニティへの参加を募る』という方針に沿って開催している.



分類	具体的な施策
フェーズ 1 (2010 年 ~2011 年)	事業部/グループ会社 IRT 窓口との連携強化 > 事業部/グループ会社 IRT と HIRT センタ連携による各種支援活動の推進 > HIRT オープンミーティングを活用した, IRT 連携の運営体制, 技術ノウハウの展開体制の整備 > セキュリティレビュー支援などから得られた課題の解決に向けた対策展開
フェーズ 2 (2012 年 ~2013 年)	IRT 連携支援メンバーとの連携強化 > IRT 連携支援メンバー (事業部・グループ会社) 制度の試行 > IRT 連携支援メンバーを起点とした IRT 活動のボトムアップ
フェーズ 3 (2014 年 ~2015 年)	バーチャルかつ横断的な対応体制の整備 > HIRT センタ~IRT 窓口~IRT 連携支援メンバーによる各種支援活動の推進 > ユーザ連携モデル (フェーズ 1, 2) と組織連携モデル (フェーズ 3) 融合による広義の HIRT (バーチャル組織体制) の構築

図 11: 日立グループ CSIRT 活動の向上

表 3: HIRT オープンミーティング『技術編』

年月	概要
2014 年 1 月	Java7 update51 セキュリティ変更点の解説 インシデント初期対応でのチェックリストを用いた調査のハンズオン
2014 年 2 月	【外部講師】 一般社団法人 JPCERT コーディネーションセンター Jack YS LIN (林 永熙) 氏 『中国のセキュリティ事情~DarKnight (中国黒客の夜明け) ~』
2014 年 3 月	【外部講師】 (株) インターネットイニシアティブ 根岸 征史氏 『監視されるインターネット』
2014 年 5 月	アドバンスド HIRT オープンミーティング
2014 年 6 月	Web サイトのセキュリティ設定ハンズオン
2014 年 8 月	Web サイトのセキュリティ設定ハンズオン 【外部講師】 トレンドマイクロ(株) 平原 伸昭氏 『標的型攻撃対策のための一般的な対応フローとビッグデータを活用したプロアクティブな対応とプロファイリングとは?』
2014 年 9 月	アドバンスド HIRT オープンミーティング
2014 年 11 月	社外サーバの脆弱性検査における技術対策セミナー

(2) 分野別 IRT 活動の試行

● HIRT-FIS におけるレディネス活動の推進

分野別視点を取り込んだインシデントレスポンス+レディネス3層サイクル(図12)を実践するため、HIRT-FIS(Financial Industry Information Systems HIRT)が主体となり、金融分野における社内外のレディネス活動を推進した。社外対応としては、金融系CSIRTとの連携を模索するためのHIRT-FISセキュリティノートの週次配信の拡大、金融系CSIRTとの意見交換会の実施を通して、日本シーサート協議会の加盟を支援した。

HIRT-FISセキュリティノートは、国内外で発生した金融関連のセキュリティインシデントや関連規則などの話題を取り上げた簡易レポートである(表4, 図13)。

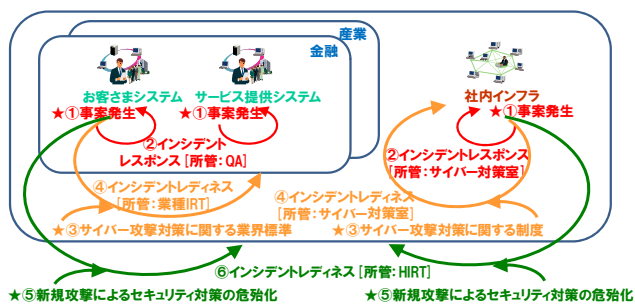


図12: インシデントレスポンス+レディネス3層サイクルの概念

表4: HIRT-FIS セキュリティノート

項目	2013年	2014年
発行数	10件	48件
受信者数	4名	9名
受信組織数	2組織	5組織

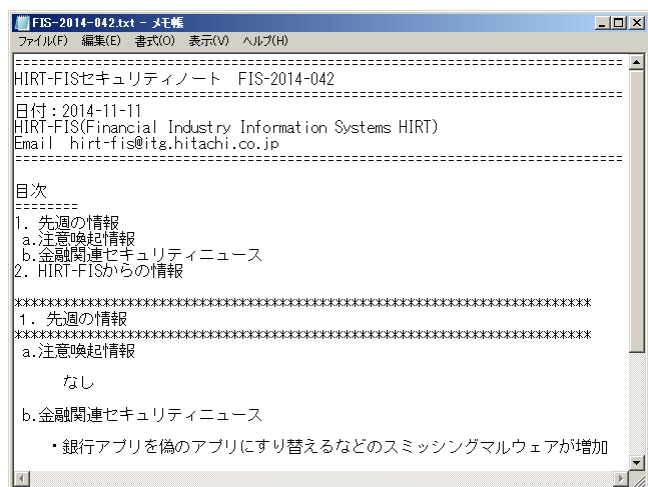


図13: 金融系CSIRT向けに週次配信しているHIRT-FISセキュリティノート

● 制御システム製品向け脆弱性対策

仕様、コード、設定の3つ視点から脆弱性対策にアプローチすると共に、コードと設定については、製品開発部署と共に、先行事例作りを推進した。

- コード: 製品の脆弱性を指摘された場合の対応について、脆弱性ハンドリングのフレームワークを加味して検討
- 設定: 米国連邦政府が推進するNCP(National Checklist Program)[6]を参考に、セキュリティ設定を整備する活動「日立チェックリストプログラム」を開始

(3) CSIRT コミュニティとの組織間連携の強化

組織間連携強化の具体的な活動として、2006年からNTT-CERT[7]と定期的に会合を開催し、CSIRT活動自身を改善するための情報交換を続けている。また、日本シーサート協議会のSSHサーバセキュリティ設定検討WGの立ち上げると共に、インシデント情報活用フレームワーク検討WGと連携し情報発信を実施した[16]。

- GNU bash の脆弱性 ~shellshock 問題~ について
- Struts: ClassLoader の操作を許してしまう脆弱性 (CVE-2014-0094, CVE-2014-0112, CVE-2014-0113) について
- OpenSSL 情報漏洩を許してしまう脆弱性 ~ Heartbleed 問題~ について

(4) その他

- MWS (マルウェア対策研究人材育成ワークショップ) 2014 への参画[11]
マルウェア対策の研究活動を支援していくと共に、支援を通して次世代のCSIRTコミュニティの醸成への寄与を目指している。
- 日経BP社ITpro CSIRTフォーラムに、脆弱性対策に関する記事「チェックしておきたい脆弱性情報」を寄稿[8]

3 HIRT

本章では、HIRTに対する理解を深めてもらうために、組織編成モデル、調整機関であるHIRTセンタの位置付け、ならびにHIRTセンタが推進している活動について述べる。

3.1 組織編成モデル

HIRTでは、4つのIRTという組織編成モデルを採用している(図14, 表5)。日立グループの場合には、情報システムや制御システムなどの製品を開発する側面(製品ベンダIRT)、その製品を用いたシ

システムを構築やサービスを提供する側面 (SIベンダIRT), そして, インターネットユーザとして自身の企業を運用管理していく側面 (社内ユーザIRT) の3つがある. 4つのIRTでは, ここに, IRT間の調整業務を行なうHIRT/CC (HIRT Coordination Center) を設けることにより, 各IRTの役割を明確にしつつ, IRT間の連携を図った効率的かつ効果的なセキュリティ対策活動を推進できると考えたモデルである. なお, HIRT という名称は, 広義の意味では日立グループ全体で推進するインシデントオペレーション活動を示し, 狭義の意味では, HIRT/CC (HIRT センタ) を示している.

実際, 4つのIRTが整備されるまでには, 表6にある4段階ほどのステップを踏んでおり, 各段階においては組織編成を後押しするトリガが存在している. 例えば, 第2ステップの製品ベンダIRT立上げにはCERT/CCから報告されたSNMPの脆弱性[9]が多く製品に影響を与えたことが後押しとなった. また, 第3ステップのSIベンダIRT立上げについては『情報セキュリティ早期警戒パートナーシップ』[29][30]の運用開始が挙げられる. HIRTセンタは, 3つのIRTの大枠が決まった後に, 社内外の調整役を担う組織として構成されたという経緯がある.

さらに, 2010年からは, バーチャルかつ横断的な対応体制を整備し, 『日立グループ全体にインシデントオペレーション活動を浸透させていくこと』を目標とした日立グループCSIRT活動の向上を推進している.

表 5 : 各 IRT の役割

分類	役割
HIRT/CC	該当部署: HIRT センタ > FIRST, 日本シーサート協議会, JPCERT/CC, CERT/CC などの社外 CSIRT 組織との連絡窓口 > SIベンダ/製品ベンダ/社内ユーザIRT組織間の連携調整
SIベンダIRT	該当部署: SI/サービス提供部署 > 顧客システムを対象とした CSIRT 活動の推進 > 公開された脆弱性について, 社内システムと同様に顧客システムのセキュリティを確保
製品ベンダIRT	該当部署: 製品開発部署 > 日立製品の脆弱性対策, 対策情報公開の推進 > 公開された脆弱性について影響有無の調査を迅速に行い, 該当する問題については, 告知と修正プログラムの提供
社内ユーザIRT	該当部署: 社内インフラ提供部署 > 侵害活動の基点とならないよう社内ネットワークのセキュリティ対策の推進

表 6 : 組織編成の経緯

ステップ	概要
1998年4月	日立としてのCSIRT体制を整備するためのプロジェクトとして活動を開始
第1ステップ 社内ユーザIRTの立上げ (1998年~2002年)	日立版CSIRTを試行するために, 日立グループに横断的なバーチャルチームを編成し, メーリングリストをベースに活動を開始. メンバ構成は主に社内セキュリティ有識者及び社内インフラ提供部門を中心に編成.
第2ステップ 製品ベンダIRTの立上げ (2002年~)	製品開発部門を中心に, 社内セキュリティ有識者, 社内インフラ提供部門, 製品開発部門, 品質保証部門等と共に, 日立版CSIRTとしての本格活動に向け, 関連事業所との体制整備を開始.
第3ステップ SIベンダIRTの立上げ (2004年~)	SI/サービス提供部門と共にSIベンダIRTの立上げを開始. さらに, インターネットコミュニティとの連携による迅速な脆弱性対策とインシデント対応の実現に向け, HIRTの対外窓口ならびに社内の各IRTとの調整業務を担うHIRT/CCの整備を開始.
2004年10月	HIRT/CCとしてHIRTセンタを設立.
2010年~	日立グループCSIRT活動の向上 目標: インシデントオペレーション活動の日立グループ全体への浸透

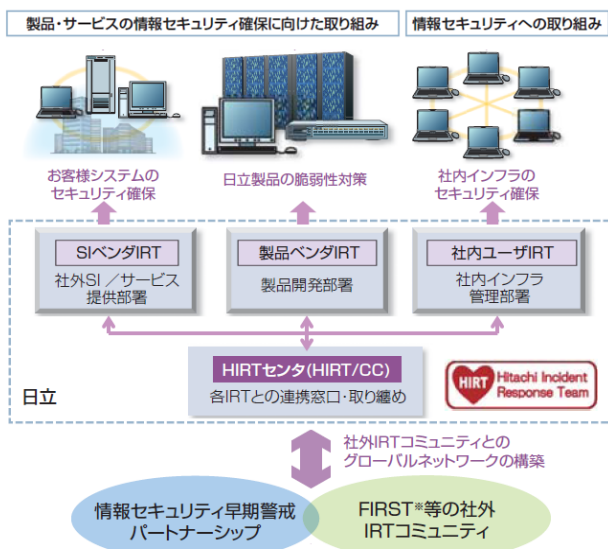


図 14 : 組織編成モデルとしての4つのIRT

3.2 HIRT センタの位置付け

HIRTセンタは, 情報・通信システム社の配下に設置されているが, 社内外の調整役だけではなく, セキュリティの技術面を牽引する役割を担っている. 主な活動は, IT戦略本部/品質保証本部との相互協力による制度面/技術面でのセキュリティ対策活動の推進, 各事業部/グループ会社への脆弱性対策とインシデント対応の支援, そして, 日立グループのCSIRT窓口として組織間連携によるセキュリティ対策活動の促進である (図15).

また、HIRT センタの組織編成上の特徴は、縦軸の組織と横軸のコミュニティが連携するモデルを採用しているところにある。具体的には、専属者と兼務者から構成されたバーチャルな組織体制をとることで、フラットかつ横断的な対応体制と機能分散による調整機能役を実現している。このような組織編成の背景には、情報ならびに制御システムの構成品が多岐にわたっているため、セキュリティ問題解決のためには、各部署の責務推進と部署間の協力が必要であるとの考えに基づく。

3.3 HIRT センタの主な活動内容

HIRT センタの主な活動には、社内向けの CSIRT 活動 (表 7) と社外向けの CSIRT 活動 (表 8) とがある。

社内向けの CSIRT 活動では、セキュリティ情報の収集/分析を通して得られたノウハウを注意喚起やアドバイザーとして発行すると共に、各種ガイドラインや支援ツールの形で製品開発プロセスにフィードバックする活動を推進している。

社内向けの注意喚起やアドバイザーの発行については、2005 年 6 月から HIRT セキュリティ情報を細分化した。注意喚起ならびに注目すべき情報を広く配布することを目的とした HIRT セキュリティ情報と、個別に対処依頼を通知する HIRT-FUP 情報とに分け、広報と優先度とを考慮した運用に移行している (表 9, 図 16)。また、情報を効果的に展開するため、情報の集約化による発行数の低減と共に、IT 戦略本部と品質保証本部と連動した情報発信を実施している。

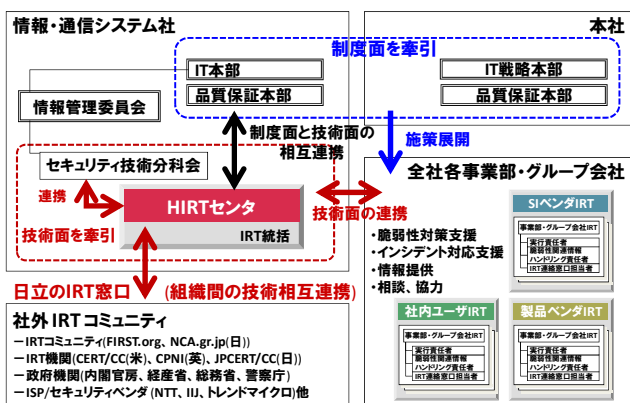


図 15 : HIRT センタの位置付け

表 7 推進中のプロジェクト (社内対応)

分類	概要
セキュリティ情報の収集/分析/提供	<ul style="list-style-type: none"> > 情報セキュリティ早期警戒対応の推進 (脆弱性対策ならびにインシデント対応に関する情報/ノウハウの水平展開) > 日立 SOCIX (Security Operation Center Information eXchange) のコンセプトに基づく広域観測網の構築
製品/サービスの脆弱性対策とインシデント対応の推進	<ul style="list-style-type: none"> > 事業部/グループ会社 IRT 窓口との連携強化 (フェーズ 3) > 脆弱性対策とインシデント対応のための技術継承 > セキュリティ情報統合サイトを活用した社外 Web サイトにおけるセキュリティ情報発信の推進
製品/サービスのセキュリティ技術の向上	<ul style="list-style-type: none"> > セキュリティ作り込みプロセスの整備 (脆弱性対策を仕様, コード, 設定の 3 つ視点からアプローチするとともに, 先行事例作りを推進)
研究活動基盤の整備	<ul style="list-style-type: none"> > 横浜研究所との共同研究体制の整備

表 8 推進中のプロジェクト (社外対応)

分類	概要
CSIRT 活動の国内連携の強化	<ul style="list-style-type: none"> > 情報セキュリティ早期警戒パートナーシップに基づく脆弱性対策活動の展開 > 日本シーサート協議会関連活動との連携
CSIRT 活動の海外連携の強化	<ul style="list-style-type: none"> > FIRST カンファレンスでの講演/参画を通じた海外 CSIRT 組織/海外製品ベンダ IRT との連携体制の整備 > 英国 WARP 関連活動の推進 > CVE, CVSS など脆弱性対策とインシデント対応の標準化 (ISO, ITU-T) への対応 [*b][10]
研究活動基盤の整備	<ul style="list-style-type: none"> > 明治大学 (菊池教授) との共同研究の推進 > マルウェア対策研究人材育成ワークショップ (MWS) [11] など学術系研究活動への参画

表 9 : HIRT が発行するセキュリティ情報の分類

識別番号	用途
HIRT-FUPyynn	優先度: 緊急 配布先: 関連部署のみ HIRT センタが日立グループ製品や Web サイトの脆弱性を発見した場合や, その報告を受けた場合など, 関連部署との連絡を必要とする際に利用する。
HIRT-yynn	優先度: 中～高 配布先: 限定なし 広く脆弱性対策とインシデント対応の注意喚起を行なう際に利用する。
HIRT-FYIynn	優先度: 低 配布先: 限定なし HIRT オープンミーティング, 講演会などの開催案内を通知する際に利用する。

*b) ISO SC27/WG3 では 2007 年から『脆弱性情報の開示 (29147) 』, 2010 年から『脆弱性対応手順 (30111) 』の検討を開始し, 2014 年 2 月, 2013 年 11 月に IS 化が完了した。ITU-T SG17 Q.4 では 2009 年から CVE (共通脆弱性識別子), CVSS (共通脆弱性評価システム) などの『サイバーセキュリティ情報交換フレームワーク (CYBEX) 』の標準化活動を推進している。

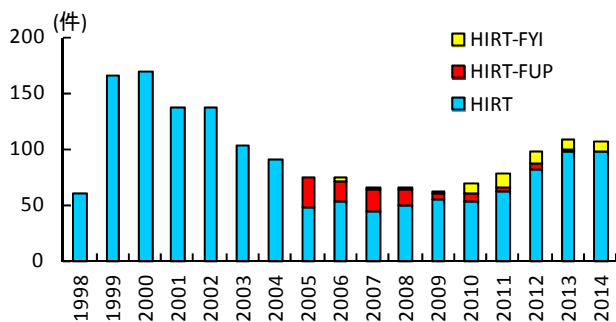


図 16：識別番号別セキュリティ情報の発行数

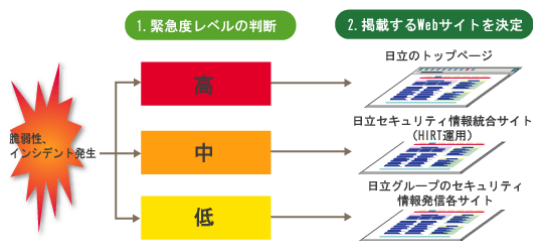


図 17：緊急度レベル×階層レベル型の情報発信の概念図

製品／サービスの脆弱性対策とインシデント対応としては、セキュリティ情報統合サイトを用いて、日立グループの製品／サービスセキュリティに関する取り組みを広くインターネットユーザに展開する活動を推進中である。特に、社外向けのセキュリティ情報の発信にあたっては、セキュリティ情報統合サイトを用いた定常的なセキュリティ情報の発信だけでなく、情報の『緊急度レベル』×掲載Webサイトの『階層レベル』とを組合せた情報発信アプローチを併用している (図 17)。

4 1998年～2013年の活動サマリ

本章では、HIRTプロジェクトとして活動を始めた1998年以降の各年の活動について述べる。

4.1 2013年

(1) 日立グループ CSIRT 活動の向上 (フェーズ 2)

4年目となる2013年は、フェーズ2の終了年として、HIRT連携支援メンバ (HIRTセンタと協力して、IRT活動を積極的に推進するメンバ) と共に、サイバーセキュリティ対策のための技術継承の場の定着化を推進した。

技術継承にあたっては、サイバー攻撃で使用されるマルウェアなどの動作の『解析』、記録された痕跡から事象を把握する『調査』、サイバー攻撃で対象となりえる脆弱性を明らかにする『評価』の3つとした。

(2) 分野別 IRT 活動の試行

● HIRT-FISにおけるレディネス活動の推進

金融分野における社外レディネス活動として、HIRT-FISセキュリティノートの週次配信の試行を開始した。

● 制御システム製品向け脆弱性対策

HIRTを対外的な窓口の基点とした脆弱性ハンドリング、インシデントハンドリングのための対応体制を整備した (図 18)[12]。

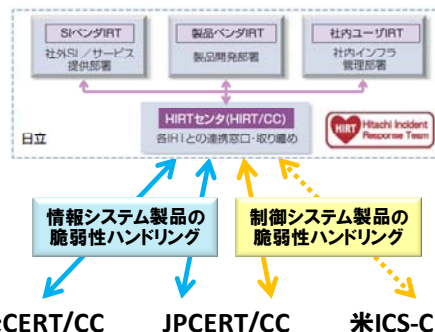


図 18：脆弱性ハンドリングのフレームワーク

(3) CSIRT コミュニティとの組織間連携の強化

日本シーサート協議会のインシデント情報活用フレームワーク検討WGと連携し情報発信を実施した[16]。

- 2013年3月から継続している国内Webサイトのページ改ざん事案について

(4) (ISC)² Asia-Pacific ISLA 2013 受賞

HIRTが携わっているJVN (Japan Vulnerability Notes) に関わる脆弱性対策活動への貢献が評価され、情報セキュリティ資格CISSPを運営する(ISC)²の2013年アジア太平洋情報セキュリティリーダーシップアチーブメントISLA (Information Security Leadership Achievements) のSenior Information Security Professionalを受賞しました[13]。

(5) その他

- MWS (マルウェア対策研究人材育成ワークショップ) 2013への参画[11]

4.2 2012年

(1) 日立グループ CSIRT 活動の向上 (フェーズ 2)

3年目となる2012年は、HIRT連携支援メンバを通じた日立グループ内連携の強化を図るフェーズ2を開始した。

- HIRTオープンミーティング『技術編』を活用した対策展開
- アドバンスドHIRTオープンミーティングの開始

(2) 分野別 IRT 活動の試行

分野別視点を取り込んだインシデントレスポンス+レディネス3層サイクルというアプローチ(図12)を取るため、分野別 IRT 活動の試行を開始した。また、金融分野における先行的な取り組みとして、2012年10月1日、金融部門内に、HIRT-FISを設置した(図19)。

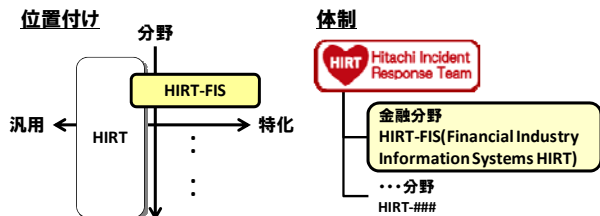


図 19: 分野別 IRT 活動の位置付けと体制

(3) CSIRT コミュニティとの組織間連携の強化

- 2012年2月29日、CSIRT活動に関心のある企業担当者を対象に、企業のCSIRTについての意見交換会の場として、CSIRTワークショップ2012を開催[14]
- 2012年11月13日～15日、国内FIRST加盟チームと共に、FIRST技術会議2012京都を京都市国際交流会館にて開催[15]
- FIRST技術会議2012京都で取り上げた『脆弱性情報のグローバルな取り扱い』を継続的に検討していくため、FIRST内にVulnerability Reporting and Data eXchange SIG (Special Interest Group) を設置

(4) 講演会

- 2012年3月：S&Jコンサルティング(株) 三輪信雄氏『組織におけるセキュリティ対策の推進体制』
- 2012年8月：日本オラクル(株) 北野晴人氏『データベース・セキュリティの要素と実装』
- 2012年9月：(独)情報通信研究機構 井上大介氏『サイバー攻撃の動向とサイバーセキュリティ研究の最先端』
- 2012年11月：NPO 情報セキュリティ研究所 上原哲太郎氏『遠隔操作事案・ファーストサーバ問題・うるう秒問題を振り返る』

4.3 2011年

(1) 日立グループ CSIRT 活動の向上 (フェーズ1)

2年目となる2011年は、フェーズ1の終了年として、事業部・グループ会社IRTと連携した支援活動サイクル(課題抽出、分析・対策検討、対策展開)の定着化に注力した。

(2) 制御システム製品の脆弱性情報の発信

制御システム製品の脆弱性報告件数が増えてきたことと、定常的に報告されている脆弱性の傾向を把握するため、制御システム製品の脆弱性をHIRTセキュリティ情報で取り上げることとした。

(3) CSIRT コミュニティとの組織間連携の強化

日本シーサート協議会のインシデント情報活用フレームワーク検討WGと連携し情報発信を実施した[16]。

- Webサービス連携を使用したWebサイト経由での攻撃mstmpについて

(4) 講演会

- 2011年7月：HASHコンサルティング(株) 徳丸浩氏『Webアプリ開発のセキュリティ要件定義』
- 2011年9月：日本アイ・ビー・エム(株) 徳田敏文氏『情報漏洩対策現場の苦勞と実務 ～悪意ある情報拡散犯の追跡～』
- 2011年12月：(株)Kaspersky Labs Japan 前田典彦氏『Androidを取り巻く状況 (Androidマルウェアの動向)』

(5) その他

- ITU-Tサイバーセキュリティ情報交換フレームワークCYBEX標準化活動への協力

4.4 2010年

(1) 日立グループ CSIRT 活動の向上 (フェーズ1)の始動

フェーズ1の初年度となる2010年は、脆弱性関連情報ハンドリング責任者/IRT連絡窓口担当者連絡会『事務編』『技術編』の定着に注力した。

- 事務編(1回/期)：脆弱性関連情報ハンドリング責任者、IRT連絡窓口担当者を対象に、IRT活動に必要な運営ノウハウの共有ならびに継承を目的とした会合
- 技術編(2～4回/期)：設計者、システムエンジニアや技術ノウハウの展開に協力して頂ける方を対象に、製品・サービスセキュリティの作り込みに必要となる技術ノウハウを展開するための会合

(2) CSIRT コミュニティとの組織間連携の強化

2010年12月に、日本シーサート協議会の国際連携ワークショップ開催を支援した。また、日本シーサート協議会のインシデント情報活用フレームワーク検討WGと連携し情報発信を実施した[16]。

- ガンブラーウイルス対策まとめサイト
- ボットネットPushDoによるSSL接続攻撃
- マルウェアStuxnet(スタクスネット)について

(3) その他

- 2010年7月、インドネシアの学術系 CSIRT 活動を支援するため、JPCERT/CC と協力して、ワークショップ『Academy CERT Meeting』の開催を後援[17]
- P2P ファイル交換ソフト環境で流通するマルウェアに関する調査[18]
P2P ファイル交換ネットワーク環境 Winny に流通するマルウェアについては、2007年以降、依然として Antinny 型の情報漏洩を引き起こす既知マルウェアが多く流通している (図 20)。

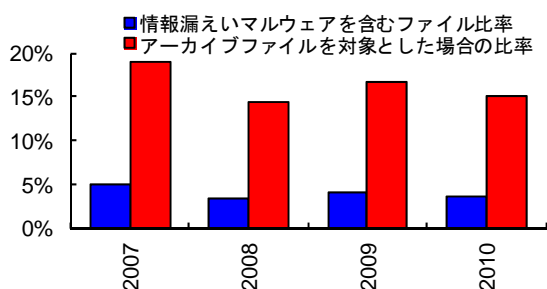


図 20 : Winny に流通する情報漏洩を引き起こすマルウェアの推移

4.5 2009 年

(1) 製品／サービスセキュリティ活動の開始

脆弱性対策とインシデント対応の活動を通じて得られたノウハウを製品開発プロセスにフィードバックするため、プロセス毎の HIRT 支援活動を開始した (図 21)。



図 21 : HIRT 支援活動の体系化

(2) セキュリティ技術者研修プログラムの実施

CSIRT 活動を活かしたセキュリティ技術者研修の一環として、グループ会社より研修生を受け入れ、Web システムのセキュリティ対策を中心とした半年間の研修を実施した。

(3) 講演会

- 2009年7月：(独)産業技術総合研究所 高木浩光氏『Web アプリケーションセキュリティ』
- 2009年7月：NTT-CERT 吉田尊彦氏『NTT-CERT の活動取り組み』

(4) その他

- P2P ファイル交換ソフト環境で流通するマルウェアに関する調査[19]
- 2009年2月：NTT-CERT 主催のワークショップにおいて、NTT グループ向けに Web アプリケーション開発の演習を実施
- 日本シーサート協議会のインシデント情報活用フレームワーク検討 WG と連携し、観測データに基づいた見える化を試みる cNotes (Current Status Notes) [20]を用いた情報発信を開始

4.6 2008 年

(1) DNS キャッシュポイズニングの対策

DNS キャッシュポイズニング対策として、『DNS の役割と関連ツールの使い方』説明会を開催した。説明会用に作成した資料は、国内の DNS キャッシュポイズニング対策に役立ててもらうため、2009年1月に IPA から発行された『DNS キャッシュポイズニング対策』[21]の資料素材として提供した。

(2) JWS2008 の開催

2008年3月25日～28日、国内 FIRST 加盟チームと共に、FIRST 技術ミーティングである FIRST Technical Colloquium と国内 CSIRT の技術交流ワークショップ Joint Workshop on Security 2008, Tokyo (JWS2008) を開催した[22]。

(3) 国内 COMCHECK Drill 2008 への参加

企業内の情報セキュリティ部署の対外向け連絡窓口のコミュニケーション確認を目的とした、国内 COMCHECK Drill 2008 (演習名：SHIWASU, 2008年12月4日実施) に参加した。

(4) 経済産業省商務情報政策局長表彰 (情報セキュリティ促進部門) 受賞

2008年10月1日、情報化月間推進会議 (経済産業省、内閣府、総務省、財務省、文部科学省、国土交通省) 主催の、平成 20 年度情報化月間記念式典において、『経済産業省商務情報政策局長表彰 (情報セキュリティ促進部門)』を受賞しました[23]。

(5) 講演会

- 2008年4月：明治大学 経営学部教授 中西晶氏『高信頼性組織のマネジメント』

(6) その他

- 新たな組織間連携の取り組みとして、標的型攻撃の実態の一旦を明らかにすべく情報処理学会コンピュータセキュリティ研究会が主催するシンポジウムの募集要項を騙ったマルウェア添付メールの検体を関連組織に提供した[24]。

4.7 2007 年

(1) 演習型 HIRT オープンミーティングの開始

ガイドライン『Web アプリケーションセキュリティガイド』のより実践的な展開を図るため、2007 年は、3 月、6 月の 2 回、Web アプリケーション開発者を対象に、演習型の HIRT オープンミーティングを開催した。

(2) 日本シーサート協議会の設立

2007 年 4 月、単独の CSIRT では解決が困難な事態に対して CSIRT 間の強い信頼関係に基づいた迅速かつ最適な対応を実施する体制作りを整備するため、IJ-SECT (IJ), JPCERT/CC, JSOC (ラック), NTT-CERT (NTT), SBSCIRT (ソフトバンク) と共に、日本シーサート協議会を設立した[25]。2014 年 12 月現在、69 チームが加盟している (図 22)。

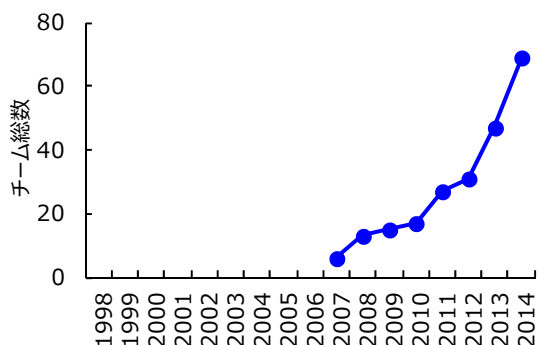


図 22：日本シーサート協議会
加盟チーム数の推移

(3) 英 WARP 加盟

2007 年 5 月、CSIRT 活動の海外連携強化のため、英国政府のセキュリティ機関 CPNI (The Centre for the Protection of the National Infrastructure) が推進する WARP (Warning, Advice and Reporting Point) に加盟した[26]。

(4) 講演会

- 2007 年 8 月：フォティーンフォティ技術研究所 鶴飼裕司氏 『静的解析による脆弱性検査』

4.8 2006 年

(1) 脆弱性届出統合窓口の設置

2006 年 11 月、日立グループにおいて脆弱性関連情報を適切に流通させ、日立のソフトウェア製品および Web サイトの脆弱性対策を推進するために、ソフトウェア製品および Web アプリケーションに関する脆弱性もしくは不具合を発見した場合の日立グループ向けの脆弱性届出統合窓口を設置した。

(2) Web アプリケーションセキュリティの強化

2006 年 10 月、日立グループにおける Web アプリケーションセキュリティ施策の一環として、ガイドラインとチェックリストを改訂すると共に、日立グループ内への展開を支援した。

(3) ファイル交換ソフトによる情報漏洩に関する注意喚起

Antinny は、2003 年 8 月に出現したファイル交換ソフトウェア『Winny』を通じて流布するマルウェアである。感染すると情報漏洩や特定サイトへの攻撃活動を発症する。HIRT では、これら脅威の状況を踏まえ、2006 年 4 月に資料『～ウィニーによる情報漏洩の防止と将来発生する危険から身を守るために～』による注意喚起を行った。

(4) 情報家電／組み込み系の製品セキュリティ活動の立上げ

情報家電／組み込み系の製品セキュリティ活動の立上げを開始した。HIRT では、インターネット電話などで用いられる通話制御プロトコルのひとつである SIP (Session Initiation Protocol) に注目し、関連するセキュリティツールならびにセキュリティ対策の状況を調査報告としてまとめた。

(5) CSIRT コミュニティとの組織間連携の強化

2006 年 3 月、NTT-CERT 主催の NTT グループ向けワークショップで日立の CSIRT 活動を紹介し、CSIRT 活動を相互に改善するための情報交換を行った。

(6) 講演会

- 2006 年 5 月：eEye Digital Security 鶴飼裕司氏 『組み込みシステムのセキュリティ』
- 2006 年 9 月：Telecom-ISAC Japan 小山覚氏 『Telecom-ISAC Japan におけるボットネット対策』

(7) その他

- HIRT から発信する技術文書 (PDF ファイル) にデジタル署名を付加する活動を開始[27]

4.9 2005 年

(1) FIRST 加盟

2005 年 1 月、各国の CSIRT 組織と連携可能なインシデント対応体制を作りながら、CSIRT 活動の実績を積むため、世界におけるコンピュータ・インシデント対応チームの国際的なコミュニティである Forum of Incident Response and Security Teams (FIRST) に加盟した[28]。加盟にあたっては、加盟済み 2 チームによる推薦が必要であり、約 1 年の準備期間を要した。

2014年12月現在、計316チームで、日本からは23チームが加盟している(図23) [*c].

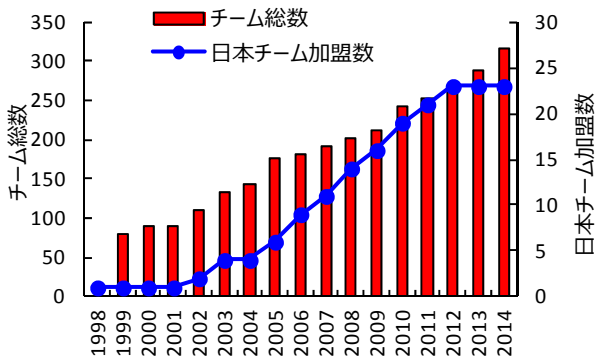


図 23 : FIRST 加盟チーム数の推移

(2) セキュリティ情報統合サイトの開設

2005年9月、日立グループの製品/サービスのセキュリティ問題に関する情報を統合的にインターネット利用者に提供するため、各事業部ならびにグループ会社のWebサイトから発信されているセキュリティ情報を統合する窓口ページを開設した(図24)。これにあわせ、セキュリティ情報発信ガイドとして『社外向けWebセキュリティ情報発信サイトの発信ガイドV1.0』を作成した。

セキュリティ情報統合サイト
 日本語 <http://www.hitachi.co.jp/hirt/>
 英語 <http://www.hitachi.com/hirt/>

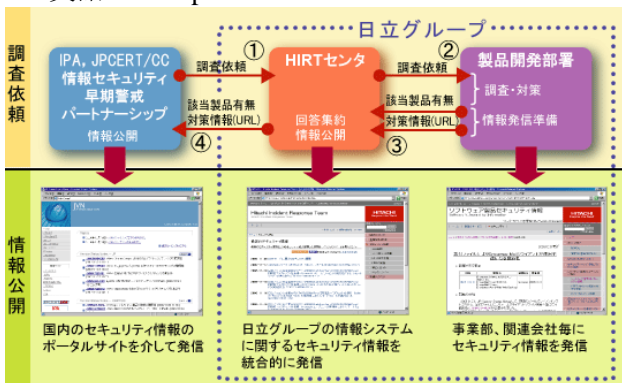


図 24 : 統合サイトでのセキュリティ情報発信

*c) CDI-CIRT(サイバーディフェンス研究所), CFC(警察庁情報通信局), DeNA CERT(DeNA), FJC-CERT(富士通), HIRT(日立), IJ-SECT(IJ), IPA-CERT(情報処理推進機構), JPCERT/CC, JSOC(ラック), KDDI-CSIRT(KDDI), KKCSIRT(カカコム), MBSD-SIRT(三井物産セキュアディレクション), MIXIRT(ミクシイ), MUFG-CERT(三菱UFJフィナンシャルグループ), NCSIRT(NRIセキュアテクノロジーズ), NISC(内閣官房情報セキュリティセンター), NTT-CERT(NTT), NTTDATA-CERT(NTTデータ), Panasonic PSIRT(パナソニック), Rakuten-CERT(楽天), RicohPSIRT(リコー), SBCSIRT(ソフトバンク), YIRD(ヤフー)

(3) CSIRT 活動の国内連携強化

CSIRT 活動の国内連携強化として、FIRST 加盟済み国内チームとの意見交換会、NTT-CERT ならびにマイクロソフト PST (Product Security Team) との個別に意見交換会を実施すると共に、Web サイト改ざん発見時の通知などの連絡網を整備した。

4.10 2004 年

(1) 情報セキュリティ早期警戒パートナーシップへの参画

2004年7月『ソフトウェア等脆弱性関連情報取扱基準』の施行にあわせて、情報セキュリティ早期警戒パートナーシップ制度が始動した[29][30]、日立グループでは、パートナーシップに製品開発ベンダとして登録(HIRTを連絡窓口)すると共に、JVN(Japan Vulnerability Notes)[31]への脆弱性対策の状況掲載を開始した。

(2) Web アプリケーションセキュリティの強化

2004年11月、Web アプリケーションの設計/開発時に留意すべき、代表的な問題点とその対策方法の概要についてまとめたWeb アプリケーションセキュリティガイドを作成し、日立グループ全体に展開した。

(3) 講演会

- 2004年1月：ISS(Internet Security Systems) Tom Noonan氏『Blaster以降の米国セキュリティビジネス事情』

4.11 2003 年

(1) Web アプリケーションセキュリティ活動の立上げ

Web アプリケーションセキュリティ強化活動の検討を開始すると共に、事業部と共同で『Web アプリケーション開発に伴うセキュリティ対策基準の作成手順』を作成した。

(2) NISCC からの脆弱性関連情報の社内展開

2002年のCERT/CC脆弱性関連情報の社内展開に続き、NISCC(現CPNI)Vulnerability Disclosure Policyに基づく脆弱性関連情報入手と情報掲載を開始した。活動開始以降、日立製品の情報がNISCC Vulnerability Advisoryに最初に掲載されたのは2004年1月の006489/H323である[32]。

(3) HIRT 社外向け連絡窓口の整備

脆弱性発見に伴う関連機関への報告と公開に関する活動の活発化にあわせ、日立製品ならびに日立が関与するサイトに対して脆弱性の存在や侵害活動の要因などが指摘された場合の対処窓口として、表10に示す連絡窓口を設置した。

表 10：連絡窓口情報

名称	"HIRT": Hitachi Incident Response Team.
所在地	〒140-8573 東京都品川区南大井 6-26-2 大森ベルポート B 館
電子メールアドレス	hirt@hitachi.co.jp
公開鍵 PGP key	KeyID = 2301A5FA Key fingerprint 7BE3 ECBF 173E 3106 F55A 011D F6CD EB6B 2301 A5FA HIRT: Hitachi Incident Response Team < hirt@hitachi.co.jp >

4.12 2002 年

(1) CERT/CC 脆弱性関連情報の社内展開

2002年にCERT/CCから報告されたSNMPの脆弱性[9]は、多くのソフトウェアや装置に影響を与えた。この脆弱性報告をきっかけに、HIRTでは、製品ベンダIRTの立上げと、CERT/CC Vulnerability Disclosure Policyに基づく脆弱性関連情報入手と情報掲載を開始した[33]。活動開始以降、日立製品の情報がCERT/CC Vulnerability Notes Databaseに最初に掲載されたのは2002年10月のVU#459371である[34]。

(2) JPCERT/CC Vendor Status Notes の構築と運用支援

国内のセキュリティ情報流通改善の試みとして、2003年2月、試行サイトJPCERT/CC Vendor Status Notes (JVN) (<http://jvn.doi.ics.keio.ac.jp/>) の構築と運用を支援した(図25)[35][36]。なお、試行サイトは、2004年7月の『ソフトウェア等脆弱性関連情報取扱基準』の施行に伴い、報告された脆弱性を公表するJapan Vulnerability Notes (JVN) サイト(<http://jvn.jp/>) にその役割を引き継がれている。

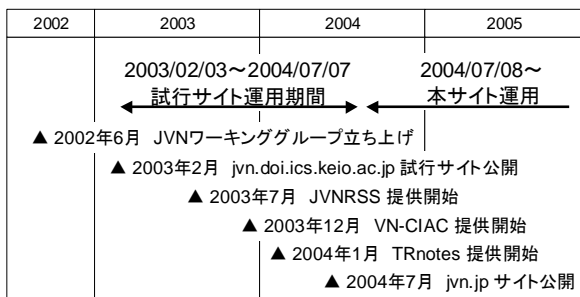


図 25：JVN 試行サイトの構築ならびに運用

4.13 2001 年

(1) Web サーバを攻撃対象とするワームの活動状況調査

インターネット上に公開している Web サーバから回収したログデータをもとに、2001年に流布した Web サーバを攻撃対象とするワームである、CodeRed I, CodeRed II, Nimda の活動状況について状況調査を実施した(2001年7月15日~2002年6月30日)。特に、国内で被害の大きかったCodeRed II, Nimda(図26)については、最初の痕跡記録時刻から最頻数となった日までわずか2日間程度であり、ワームによる被害波及が短期間かつ広範囲に渡っていた。

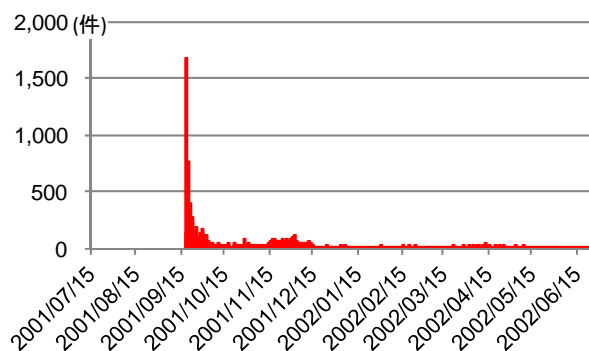


図 26：観測期間内の痕跡数変位 (Nimda)

4.14 2000 年

(1) 脆弱性の深刻度に関する指標調査

侵害活動などに利用される脆弱性の深刻度を図るために、関連機関が提示している脆弱性の深刻度の指標を調査した。

CERT/CCでは、脆弱性毎にVulnerability Notes[37]と呼ぶメモを作成し、その中で脆弱性の深刻度を示すSeverity Metricsを算出している[38]。MITREが推進するCVE(共通脆弱性識別子)では脆弱性を『通常考えられる一般的なセキュリティポリシーを侵害するVulnerability』と『個々の環境に依存し、個別のセキュリティポリシーを侵害するExposure』の2つに区別し、Vulnerabilityを脆弱性として取り扱う[39]。また、NISTでは、NVDの前身であるICAT Metabase[40]において、CERTアドバイザリならびにCVEの発行有無を脆弱性の深刻度判定の目安とし、3段階の分類を行っている。

なお、各組織で使用する脆弱性の深刻度指標が異なっていることから、2004年、脆弱性の深刻度を包括的かつ汎用的に評価する共通指標としてFIRSTが推進するCVSS(共通脆弱性評価システム)[41]が利用され始めた。

4.15 1999年

(1) hirt.hitachi.co.jp ドメイン稼働開始

日立グループへのセキュリティ情報提供の改善を図るため、1999年12月、HIRTプロジェクト用の社内向けドメインを用意し、Webサイト hirt.hitachi.co.jp を上げた。

(2) Web サイト書き換えの調査

1996年に米国でWebサイトのページ書き換えが発生してからネットワークワーム世代(2001年～2004年)までの間、Webサイトのページ書き換えが代表的なインシデントとなった。1999年～2002年にかけて、侵害活動の発生状況を把握するために、Webサイトのページ書き換えに関する調査を行なった(図27)。

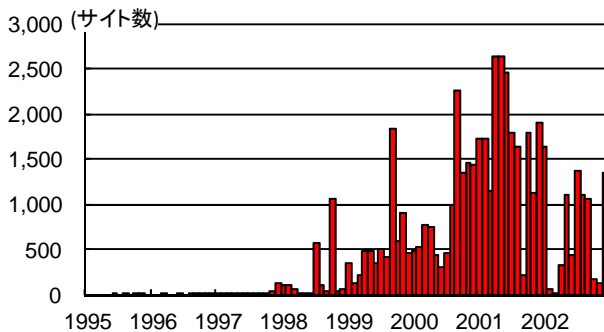


図 27 : Web サイトの書き換え件数の推移

4.16 1998年

(1) HIRT セキュリティ情報のサービス開始

1998年4月、CERT/CC、JPCERT/CCや製品ベンダ(シスコ、ヒューレッド・パッカード、マイクロソフト、ネットスケープ、サン・マイクロシステムズなど)が発行するセキュリティ情報を元に社内メーリングリストとHIRTプロジェクト用の社内Webサイトにて対策情報の提供を開始した。

(2) ネットワークセキュリティセミナー開催

1998年6月25日～26日、米セキュリティカンファレンスDEFCON[42]にスピーカとしても参加している米国技術者を講師に迎え、日立向けに『ネットワークセキュリティ』教育を実施した。

5 おわりに

情報システムや制御システムをベースにインターネットを活用して構築された社会インフラは、インシデントにつながる脅威の一つとして、脆弱性という課題に直面している。そして、日々のサイバー対策活動を通して、新たな脅威と成り得る脆弱性という課題に立ち向かっていく必要がある。

HIRTでは、新たな脅威に対処するために、『次の脅威をキャッチアップする』過程の中で、早期に対策展開を図る活動を進めていく。また、分野に特化したCSIRT活動の推進、次世代のCSIRTコミュニティにつながる学術系との場の醸成などを通して、安心、安全な社会インフラの実現に寄与していく。

(2015年8月13日)

参考文献

- 1) 警察庁, 平成 26 年中のインターネットバンキングに係る不正送金事犯の発生状況等について, http://www.npa.go.jp/cyber/pdf/H270212_banking.pdf
- 2) Symantec, 2015 Internet Security Threat Report, Vol. 20 http://www.symantec.com/security_response/publications/threatreport.jsp
- 3) Arbor Networks, ATLAS Q3 2014 DDoS Attack Trends http://www.slideshare.net/Arbor_Networks/atlas-q3-2014-ddos-attack-trends
- 4) NIST, NVD (National Vulnerability Database), <http://nvd.nist.gov/>
- 5) (独)情報処理推進機構, 脆弱性関連情報に関する届出状況, <https://www.ipa.go.jp/security/vuln/report/press.html>
- 6) NIST, National Checklist Program <http://www.nist.gov/itl/csd/scm/ncp.cfm>
- 7) NTT-CERT (NTT Computer Security Incident Response and Readiness Coordination Team), <http://www.ntt-cert.org/>
- 8) ITpro セキュリティ, <http://itpro.nikkeibp.co.jp/security/>
- 9) CERT Advisory CA-2002-03, "Multiple Vulnerabilities in Many Implementations of the Simple Network Management Protocol (SNMP)" (2002/2), <http://www.cert.org/advisories/CA-2002-03.html>
- 10) HIRT-PUB14008: サイバーセキュリティ情報交換フレームワーク CYBEX, <http://www.hitachi.co.jp/hirt/publications/hirt-pub14008/index.html>
- 11) マルウェア対策研究人材育成ワークショップ, <http://www.iwsec.org/mws/2015/>
- 12) HIRT-PUB10008: 日立グループにおける製品脆弱性情報の開示プロセス (2010/9), <http://www.hitachi.co.jp/hirt/publications/hirt-pub10008/index.html>
- 13) (ISC)² Information Security Leadership Achievements (ISLA)プログラム, <https://www.isc2.org/japan/isla.html>
- 14) CSIRT ワークショップ 2012, <http://www.hitachi.co.jp/hirt/topics/20120229.html>
- 15) Kyoto 2012 FIRST Technical Colloquium, <http://www.first.org/events/colloquia/kyoto2012>
- 16) 日本シーサート協議会, インシデント対応まとめサイト, <http://www.nca.gr.jp/2010/incidentresponse.html>
- 17) SGU MIT Workshop Academy CERT Meeting (2010/7), <http://academy-cert-indonesia.blogspot.jp/2010/06/academy-cert-meeting.html>
- 18) HIRT-PUB11003: P2P ファイル交換ソフト環境で流通するマルウェア (2011年)(2011/9), <http://www.hitachi.co.jp/hirt/publications/hirt-pub11003/index.html>
- 19) HIRT-PUB09008: 2009 年ファイル交換ソフトによる情報漏えいに関する調査結果 (2009/12), <http://www.hitachi.co.jp/hirt/publications/hirt-pub09008/index.html>
- 20) cNotes: Current Status Notes, <http://jvnrss.ise.chuo-u.ac.jp/csn/index.cgi>
- 21) (独)情報処理推進機構, DNS キャッシュポイズニング対策 (2009/2), https://www.ipa.go.jp/security/vuln/DNS_security.html
- 22) Joint Workshop on Security 2008, Tokyo 開催記録サイト (2008/3), <http://www.nca.gr.jp/jws2008/index.html>
- 23) 情報化月間 2008-平成 20 年度情報化促進貢献企業等表彰 (2008/10), http://www.meti.go.jp/policy/it_policy/gekkan/#gekkan_kako
- 24) (一社)情報処理学会, 情報処理: マルウェア: 5. コラム: 標的型メールがやってきた (2010/3), https://ipsj.ixsq.nii.ac.jp/ej/?action=repository_&uri&item_id=69232&file_id=1
- 25) 日本シーサート協議会, <http://www.nca.gr.jp/>
- 26) WARP (Warning, Advice and Reporting Point), <http://www.warp.gov.uk/>
- 27) GlobalSign Adobe Certified Document Services, <https://jp.globalsign.com/solution/example/hitachi.html>
- 28) FIRST (Forum of Incident Response and Security Teams), <http://www.first.org/>
- 29) 経済産業省告示第 235 号, ソフトウェア等脆弱性関連情報取扱基準 (2004/7), <http://www.meti.go.jp/policy/netsecurity/vulhandlingG.html>
- 30) (独) 情報処理推進機構, 情報セキュリティ早期警戒パートナーシップガイドライン (2004/7), https://www.ipa.go.jp/security/ciadr/partnership_guide.html
- 31) JVN (Japan Vulnerability Notes), <http://jvn.jp/>
- 32) NISCC, NISCC Vulnerability Advisory 006489/H323: Vulnerability Issues in Implementations of the H.323 Protocol (2004/1), <http://www.kb.cert.org/vuls/id/JSHA-5V6H7S>
- 33) CERT/CC Vulnerability Disclosure Policy, http://www.cert.org/kb/vul_disclosure.html
- 34) US-CERT, Vulnerability Note VU#459371: "Multiple IPsec implementations do not adequately validate authentication data" (2002/10), <http://www.kb.cert.org/vuls/id/459371>
- 35) JPCERT/CC Vendor Status Notes DB 構築に関する検討, CSS2002 (2002/10), <http://www8.cao.go.jp/cstp/project/export/ITPT-B/ITPT1/shiryu.1-6.pdf>
- 36) セキュリティ情報流通を支援する JVN の構築 (2005/5), <http://www.hitachi.co.jp/hirt/csirt/jvn/index.html>
- 37) CERT/CC Vulnerability Notes Database, <http://www.kb.cert.org/vuls>
- 38) CERT/CC Vulnerability Note Field Descriptions, <http://www.kb.cert.org/vuls/html/fieldhelp>
- 39) CVE (Common Vulnerabilities and Exposures), <http://cve.mitre.org/>
- 40) ICAT, <http://icat.nist.gov/> (not available)
- 41) CVSS (Common Vulnerability Scoring System), <http://www.first.org/cvss/>
- 42) DEFCON, <http://www.defcon.org/>

執筆者

寺田真敏(てらだ まさと)
 1998 年に HIRT の活動を立ち上げて以降, 2002 年に JVN (<http://jvn.jp/>) の前身となる研究サイト (<http://jvn.doi.ics.keio.ac.jp/>) の立ち上げ, 2005 年には HIRT の窓口として CSIRT の国際団体である FIRST への加盟など対外的な CSIRT 活動を推進。現在, JPCERT コーディネーションセンター専門委員, (独) 情報処理推進機構研究員, テレコム・アイザック推進会議運営委員, 日本シーサート協議会の運営委員長を務める。